

## ABSTRACT

The present invention offers a prime calculating apparatus for calculating a prime which can be determined whether it has been duly  
5 generated. The prime calculating apparatus (i) generates a random number, (ii) calculates a multiplication value R by multiplying a management identifier by the random number, and (iii) calculate a prime candidate N, according to  $N = 2 \times (\text{multiplication value } R + w) \times \text{prime } q + 1$ , with respect to w satisfying an equation of  $2 \times w \times \text{prime } q + 1 = \text{verification value (mod management information)}$ . Then, the prime  
10 calculating apparatus judges whether the calculated prime candidate N is a prime, and outputs the calculated prime candidate N as a prime when determining that it is a prime.

15